NAME : Miguel Á. Sánchez	GROUP REF. : SC D2
COUNTRY : Spain	PREF. SUBJECT : PS2
REGISTRATION NUMBER : 219711391	QUESTION N° : Q2.11

As manufacturers of equipment for the electricity sector, we are aware that every functionality or solution, whether new or evolving, must be tested by EPUs to ensure interoperability and detect possible unexpected effects on the electrical infrastructure.
In the case of cyber security, new situations are introduced, which may have effects that are not visible at first glance, such as the difficulty of operating a critical system under emergency conditions, for example due to the expiration of the operator's password, or the difficulty of entering it in certain interfaces.
This means that many EPUs have to define specific requirements to adapt the solutions to their systems and internal processes, which leads manufacturers to a particularization that, although at a functional level may represent a competitive advantage, at a cybersecurity level it is usually the opposite, since if not all suppliers have it, this solution or requirement may be eliminated.
In the electrical sector, the existence of a standard certification scheme is very valuable, as it is already applied for other characteristics such as electromagnetic immunity or environmental characteristics. Whether at the European or Global level, so that the huge efforts needed to implement cybersecurity solutions by the entire supply chain are common and available for use by all EPUs. In addition, we believe that a standard certification framework, adapted to the needs of the sector (e.g. more lightweight than Common Criteria), allows to reduce the tests that have to be performed almost independently by each EPU right now, so that we can obtain more cybersecurity guarantees with much less cost. But it does not eliminate the need to perform some tests in their systems.
Taking as a reference the IEC 62351-100 series, which defines standard test cases, and IEC 62443-4-1 and IEC 62443-4-2, or the ongoing work on IEC 62443-6, we have a very good basis for establishing a certification system adapted to the electricity sector, to achieve an adequate level of cybersecurity in all layers of the infrastructure, which is easy to adapt to the risk estimation of each EPU. We could take as an example the work being done for many years with IEC 61850, in which through certifications (Edition 1, Edition 2, ...) IEDs are deployed, problems and situations not contemplated in the standard are surfaced, and they are solved, defining real substation use cases and adapting the certifications.
In Europe, ENISA is in charge of defining a cybersecurity certification framework at European level (EUCC), and this framework must take into account the sectoral regulations, in order to adapt it to the energy sector. This framework should provide an agile way to incorporate new requirements, either due to new technologies as they emerge, or due to lessons learned from incidents as they occur.